CYBER SECURITY NEWS
Vol. 6 | Issue 11
November 2021

Page 2 | Page 3 | Challenge | Closing

Welcome to the TXDPS Cyber Security Newsletter!

It's pretty much fall, y'all! I know it's hard to tell because, well, Texas...but I think it's finally here! Hope this newsletter finds you and your families doing well as we head into the holiday season.

Let's kick this newsletter off with a bit of a confession. You may have recently noticed a wave of different emails that seemed phishy or weird. One was about an eCard; one was a LinkedIn friend request; and the latest one mentioned computer updates from IT. Well...they were from our Cyber Ops team. (A few of you snuffed this out quickly!)

First, please know that we weren't out to "get you" or make you feel bad or panic. Our intention is never to lure you into bad situations so we can berate you with finger wags.

We ran this simulated phishing baseline as part of Cybersecurity Awareness Month to determine how our agency would react if a real phishing attack were to occur. And, I have to say, many of you made a Cyber Training Officer proud! We had many people raise the alarm and warn other team members about the possible attack. Well done!

In addition to our annual awareness training and monthly newsletters, we will continue to send out simulated phishing tests so we can all practice the skills of identifying and reporting phishing emails. Ideally, we will see an increase in reported emails and a decrease in clicks. Remember, both links *and* attachments can be malicious. And, replying to an email can be just as dangerous.

To properly report a suspicious email message, please forward the email as an attachment to our spam mailbox. If the email is part of a simulated phish campaign, our dashboard will capture that you reported it, and you'll be receiving kudos from our team. If it's a real phish, forwarding it to that inbox will allow our analysts to check it out and follow up as necessary. They'll also be able to track trends and identify patterns as well as update their security tools to fortify our email system.

Thank you for slowing down when receiving email and looking for red flags. If you need a reminder about what phishing even is or help with what all the red flags are, please reach out to me for a crash refresher. Don't get hooked!

Cyber Risk Management

Slow your roll and know your role!

In this month's Risk Management section we're focusing on handling DPS data and what your responsibilities are as an employee. When it comes to handling DPS data everyone has a role to play. The question is, do you know yours? Before you dig into those Thanksgiving rolls, let's take a look at some of the data roles and where you fit in. Keep in mind, you may belong to more than one!

Note: The descriptions below are focused on data within an information system, but data security also applies to physical hardcopies as well (so keep those desks clean and those file cabinets locked!).

Data Owner – If you are a Data Owner, it means you have operational authority for the data and are responsible for the overall procurement, operation, and maintenance of the associated information system. You are not necessarily doing the day-to-day work, but you are responsible for making sure that the necessary work is taking place. Data Owners must make sure to work with Cyber Security on determining security requirements for their systems, communicate the security requirements to the Data Custodians, and provide justification and approval for any security control exceptions. Since this doesn't apply to most of you, let's keep reading!

Data Custodian – If you are a Data Custodian, it means you are responsible for the day-to-day management of data within an information system. You work with the Data Owner and Cyber Security to understand and implement the appropriate security requirements and report any security concerns. This could mean you are an Administrator for a system within your Division, IT personnel conducting system backups and vulnerability remediations, or even a third-party vendor that provides maintenance or hosting services. You might be responsible for granting permissions to an application, reviewing user accounts, or configuring application settings. All of these scenarios mean that you need to be aware of the data security requirements of a system so that we don't end up out of compliance. Still doesn't apply to you? Then let's look at one more role.

Data User – If you are a Data User, it means you have been granted access to the data for day-to-day business purposes. You are responsible for using the data only as needed to do your job and making sure to comply with requirements when it comes to how this data is shared or disseminated. Even as a User, it's important to understand the Data Classification and DPS security policies to prevent unauthorized or accidental disclosure. This is where most of you readers will fall. Hopefully by now you have found your role!

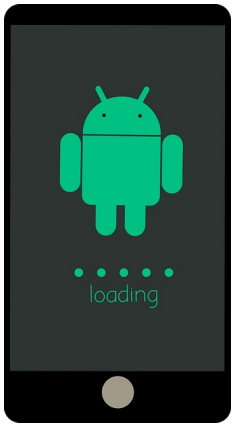
We know this can be confusing, but don't forget this information can always be found in GM Chapter 25 (the Cyber Security chapter). And in case you were wondering, we didn't make this up ourselves. Information on roles and responsibilities can also be found in Texas Administrative Code (TAC) chapter 202 As always, feel free to reach out to us if you have questions or just want to chat about security.

Now go enjoy some Thanksgiving rolls!

In the News

This New Android Malware Can Gain Root Access to Your Smartphones

(Ravie Lakshmanan | October 29, 2021)



An unidentified threat actor has been linked to a new Android malware strain that features the ability to root smartphones and take complete control over infected smartphones while simultaneously taking steps to evade detection.

The malware has been named "AbstractEmu" owing to its use of code abstraction and anti-emulation checks undertaken to thwart analysis right from the moment the apps are opened. Notably, the global mobile campaign is engineered to target and infect as many devices as possible indiscriminately.

Lookout Threat Labs said it found a total of 19 Android applications that posed as utility apps and system tools like password managers, money managers, app launchers, and data saving apps, seven of which contained the rooting functionality. Only one of the rogue apps, called Lite Launcher, made its way to the official Google Play Store, attracting a total of 10,000 downloads before it was purged.

The apps are said to have been prominently distributed via third-party stores such as the Amazon Appstore and the Samsung Galaxy Store, as well as other lesser-known marketplaces like Aptoide and APKPure.

"While rare, rooting malware is very dangerous. By using the rooting process to gain privileged access to the Android operating system, the threat actor can silently grant themselves dangerous permissions or install additional malware — steps that would normally require user interaction," Lookout researchers said. "Elevated privileges also give the malware access to other apps' sensitive data, something not possible under normal circumstances."

Once installed, the attack chain is designed to leverage one of five exploits for older Android security flaws that would allow it to gain root permissions and take over the device, extract sensitive data, and transmit to a remote attack-controlled server

Lookout attributed the mass distributed rooting malware campaign to a "well-resourced group with financial motivation," with telemetry data revealing that Android device users in the U.S. were the most impacted. The ultimate objective of the infiltrations remains unclear as yet.

"Rooting Android or jailbreaking iOS devices are still the most invasive ways to fully compromise a mobile device," the researchers said, adding "mobile devices are perfect tools for cyber criminals to exploit, as they have countless functionalities and hold an immense amount of sensitive data."

Full Story: https://thehackernews.com/2021/10/this-new-android-malware-can-gain-root.html

A Few More Cyber News Stories:

Microsoft to work with community colleges to fill 250,000 cyber jobs
https://www.reuters.com/technology/microsoft-work-with-community-colleges-fill-250000-cyber-jobs-2021-10-28/

Teen Rakes in $2.74M Worth of Bitcoin in Phishing Scam
https://threatpost.com/teen-rakes-in-2-74m-worth-of-bitcoin-in-phishing-scam/175834/

Scammers are emailing waves of unsolicited QR codes, aiming to steal Microsoft users' passwords
https://www.cyberscoop.com/qr-code-phishing-scam/

CYBER CHALLENGE

Cyber Trivia

This Month's Challenge

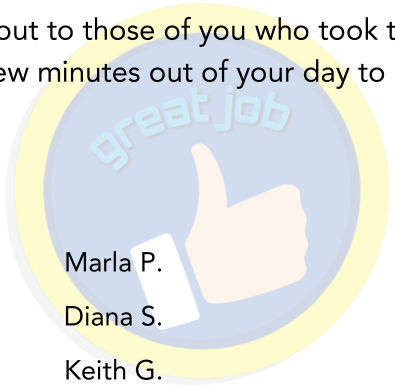
For this month's challenge, let's play a little Cyber Trivia!

To get started, click the wheel below. Let me know when you've knocked out each category. And I'm also curious which one you struggled with the most.

Good luck! (~10-15 minutes to complete)

Closing Comments

As we close this month's newsletter, we'd like to give a quick shout out to those of you who took the time to engage with our cyber challenge. We fully appreciate you taking a few minutes out of your day to engage with us. Please keep doing so; and get others to join you.



A big THANK YOU to:

Justin G.	Joyce S.	Marla P.
Kalyn B.	Jennifer P.	Diana S.
Debra L.	SJ J.	Keith G.
Patricia G.	Elaine D.	Lance J.
Linda P.	Abigail R.	Amber D.
Cindy G.	Jessica B.	Butch D.
Stacey P.	Vantrice J.	

If we missed you, let us know!

Thank you to all who participated in our Cybersecurity Awareness Month activities! We had lots of great interactions, questions, and discussions. I sincerely hope we can keep the conversation going year-round.

Now the moment of truth….. Congrats to our winners of our two raffles!

Amazon/Starbucks Gift Card Winners (from Interactive Game):

- Karyn
- Elizabeth
- Eloisa

Yeti Tumbler Winner (from Scavenger Hunt):

- Lane

I will be contacting each of you individually to follow up on how to get your prize. Thanks again to all who participated. I hope to do more stuff like this in the near future. Stay tuned!

As always, I'm open to feedback on anything and everything cyber-awareness related. Don't hesitate to reach out to me. Thank you all for your continued cyber diligence! Have a great Thanksgiving break!

-Eric Posadas